''sale'' to the acquisition of similar items.

(2) Include the following additional information with the SF 120:

(i) The identity of the offeror of the exchange;

(ii) The type of replacement equipment;

(iii) The acquisition method for the replacement equipment;

(iv) The anticipated purchase price for the replacement equipment; and

(v) The name and telephone number of the contracting officer.

(g) Evaluate offers using the solicitation criteria, including consideration of any exchange allowance offers. Award can be made whether or not the replaced information technology is exchanged.

(h) Before a contract is awarded, consider the results of the screening. Do not make an exchange if another Government agency wants to acquire the replaced equipment.

(1) If another agency is going to acquire the replaced equipment, do not include the exchange allowance in the contract price.

(2) The actual sale price to the agency acquiring the replaced equipment will be the exchange allowance (if any) of the successful offeror.

(i) If no Government agency wants to acquire the replaced equipment, the contract price shall include the exchange allowance, if any.

(j) If no exchange allowance was offered by the successful contractor, see the Defense Automation Resources Management Manual for disposal instructions.

[62 FR 1059, Jan. 8, 1997, as amended at 62 FR 34127, June 24, 1997; 62 FR 49305, Sept. 19, 1997]

Subpart 239.71—Security and Privacy for Computer Systems

SOURCE: 69 FR 35534, June 25, 2004, unless otherwise noted.

239.7100 Scope of subpart.

This subpart includes information assurance and Privacy Act considerations. Information assurance requirements are in addition to provisions concerning protection of privacy of individuals (see FAR Subpart 24.1).

239.7101 Definition.

Information assurance, as used in this subpart, means measures that protect and defend information, that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed, and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

239.7102 Policy and responsibilities.

239.7102–1 General.

(a) Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes, to include—

(1) The National Security Act;

(2) The Clinger-Cohen Act;

(3) National Security Telecommunications and Information Systems Security Policy No. 11;

(4) Federal Information Processing Standards;

(5) DoD Directive 8500.1, Information Assurance; and

(6) DoD Instruction 8500.2, Information Assurance Implementation.

(b) For all acquisitions, the requiring activity is responsible for providing to the contracting officer—

(1) Statements of work, specifications, or statements of objectives that meet information assurance requirements as specified in paragraph (a) of this subsection;

(2) Inspection and acceptance contract requirements; and

(3) A determination as to whether the information technology requires protection against compromising emanations.

239.7102–2 Compromising emanations—TEMPEST or other standard.

For acquisitions requiring information assurance against compromising emanations, the requiring activity is responsible for providing to the contracting officer—